nic.br cgi.br | 20 anos cert.br

Em dia com a Segurança da Informação
CEMIG, Belo Horizonte, MG
23/11/17

cgi.br

1 2 3 4 5 6 7 8 9 — GOVERNO e 10 11 12 13 14 15 16 17 18 19 20 21 — SOCIEDADE CIVIL

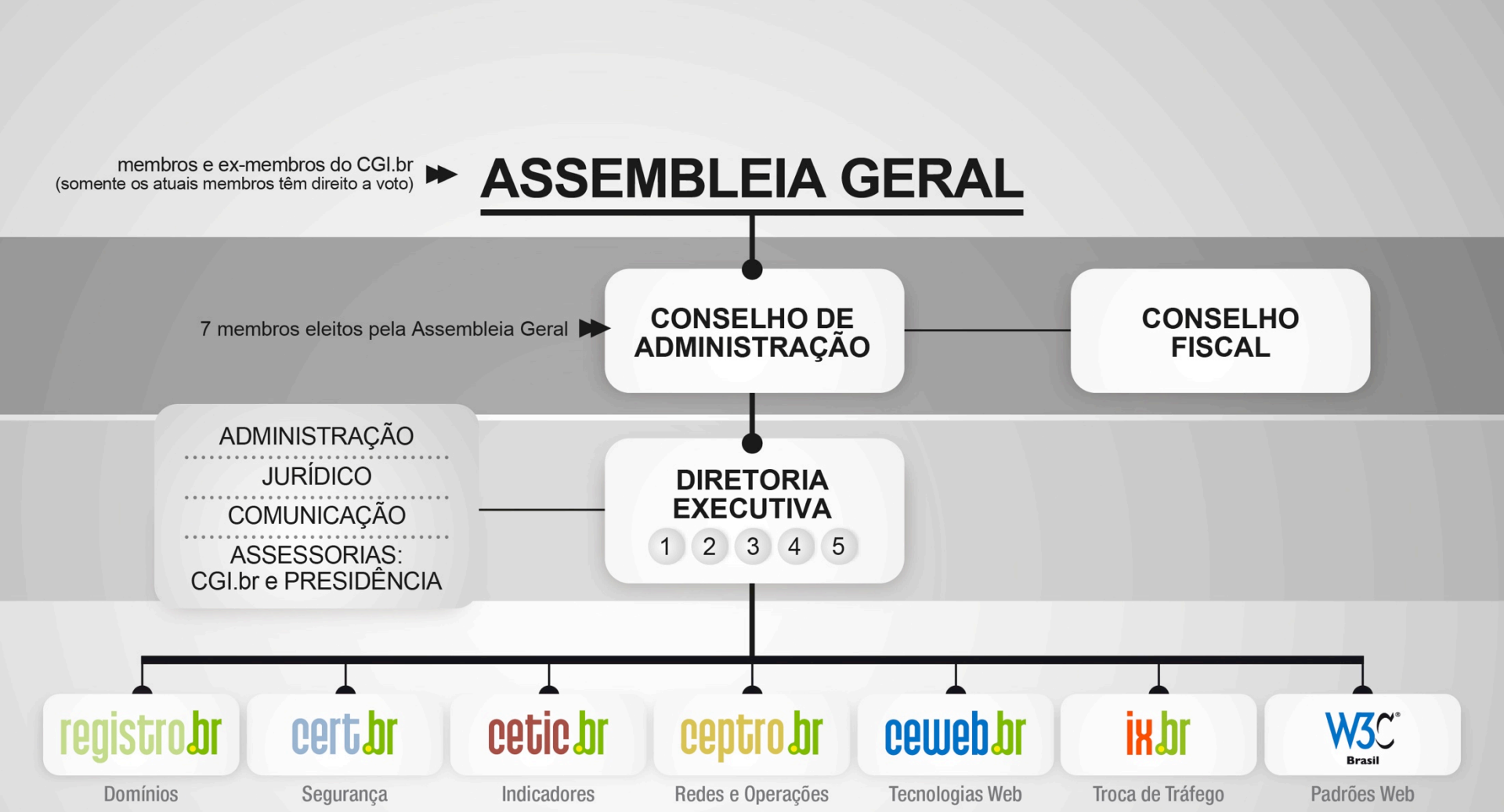
Representantes do Governo:

1 Ministério da Ciência, Tecnologia e Inovação (coordenador)
2 Casa Civil da Presidência da República
3 Ministério das Comunicações
4 Ministério da Defesa
5 Ministério do Desenvolvimento, Indústria e Comércio Exterior
6 Ministério do Planejamento, Orçamento e Gestão
7 Agência Nacional de Telecomunicações
8 Conselho Nacional de Desenvolvimento Científico e Tecnológico
9 Conselho Nacional de Secretários Estaduais para Assuntos de Ciência e Tecnologia

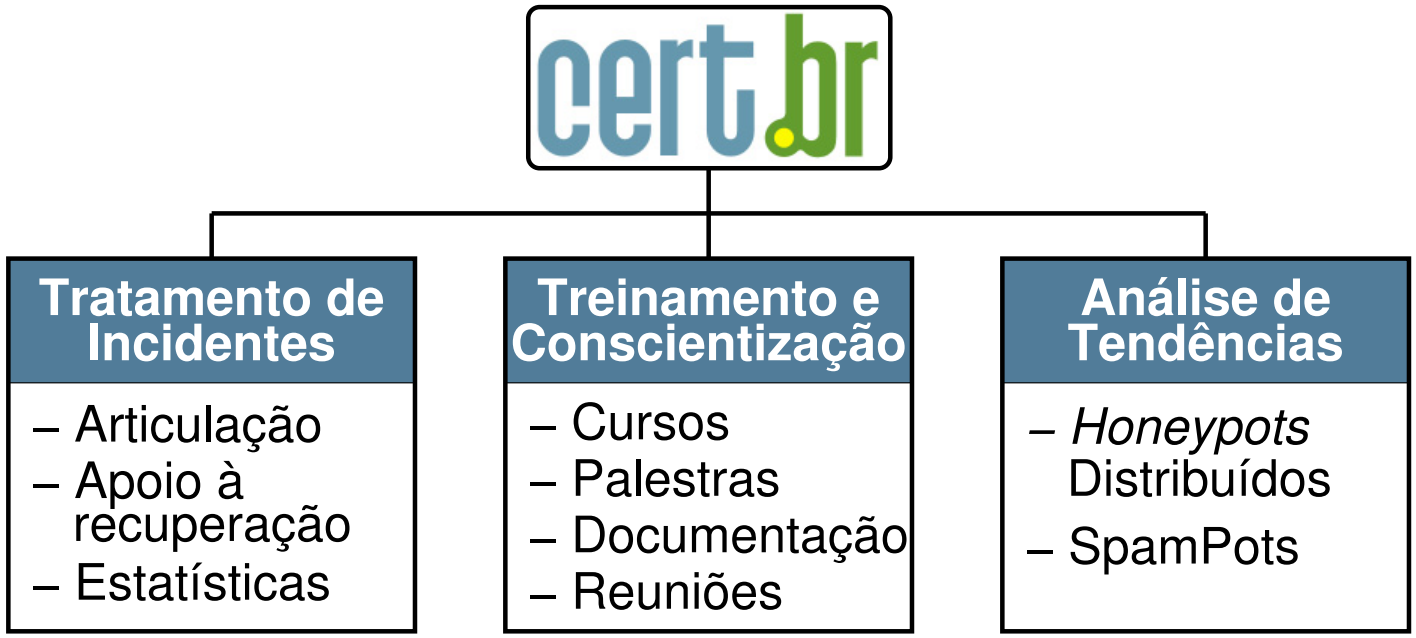
Representantes da Sociedade Civil:

10 Notório saber em assunto da Internet
11 a 14 Representantes do setor empresarial
- provedores de acesso e conteúdo da Internet
- provedores de infra-estrutura de telecomunicações
- indústria de bens de informática, de bens de telecomunicações e de software
- setor empresarial usuário

15 a 18 Representantes do terceiro setor
19 a 21 Representantes da comunidade científica e tecnológica



1 Diretor presidente
2 Diretor administrativo e financeiro
3 Diretor de serviços e de tecnologia
4 Diretor de projetos especiais e de desenvolvimento
5 Diretor de assessoria às atividades do CGI.br



SEI Partner
Carnegie Mellon

FIRST
Improving Security Together
MEMBER

APWG
RESEARCH PARTNER
www.antiphishing.org

The Honeynet PROJECT

Criado em 1997 para:

- **Ser um ponto de contato nacional para notificação de incidentes**
- **Prover a facilitação e o apoio necessários no processo de resposta a incidentes**
- **Estabelecer um trabalho colaborativo com outras entidades**
- **Aumentar a conscientização sobre a necessidade de segurança na Internet**
- **Auxiliar novos CSIRTs (Grupos de Tratamento de Incidentes de Segurança) a estabelecerem suas atividades**

Ransomware: Proteger seus arquivos nunca foi tão importante!

Miriam von Zuben
miriam@cert.br

cert.br nic.br cgi.br

Ransomware (1/5)

Tipo de código malicioso que torna inacessíveis os dados armazenados em um equipamento, geralmente usando criptografia, e que exige pagamento de resgate (*ransom*) para restabelecer o acesso ao usuário

Ransomware (2/5)

- **Tipo de código malicioso**
  - como vírus, *trojan*, *backdoor*, *worm*, *bot* e *spyware*

- **Pode infectar:**
  - computadores (*desktops*, *notebooks*, servidores)
  - equipamentos de rede (*modems*, *switches*, roteadores)
  - dispositivos móveis (*tablets*, celulares, *smartphones)*

Ransomware (3/5)

- **Infecção ocorre pela execução de arquivo infectado:**
  - recebido:
    - via *links* em *e-mails*, redes sociais e mensagens instantâneas
    - anexado a *e-mails*
  - baixado de *sites* na Internet
  - acessado:
    - via arquivos compartilhados
    - via páginas Web maliciosas, usando navegadores vulneráveis
- **Não se propaga sozinho**

Ransomware (4/5)

- **Ações mais comuns**
  - impede o acesso ao equipamento (*Locker ransomware*)
  - impede o acesso aos dados armazenados no equipamento, geralmente usando criptografia (*Crypto ransomware*)

- **Extorsão é o principal objetivo dos atacantes**
  - pagamento feito geralmente via *bitcoins*
  - não há garantias de que o acesso será restabelecido
    - mesmo que o resgate seja pago
  - normalmente usa criptografia forte
  - instigam medo e pânico na vítima

Ransomware (5/5)

- **Impacto:**
  - perdas financeiras
    - pagamento do resgate
    - tempo de recuperação
    - serviços indisponíveis
  - danos a reputação

- **Costuma:**
  - apagar arquivos de *backup*
  - buscar outros dispositivos conectados, locais ou em rede, e criptografá-los também
  - cifrar arquivos na nuvem

História – Origem

- **AIDS, Aids Info Disk, PC Cyborg Trojan (Cryptoviral)**
  - 1989, considerado o primeiro
  - passava-se por licença de *software* expirada
  - criptografava os nomes dos arquivos no drive C:
  - usava criptografia simétrica senha (contida no próprio código)
  - pagamento via cheque para conta no Panamá
  - cenário na época
    - computadores não tão difundidos (poucos usuários)
    - pagamentos internacionais não tão fáceis e comuns
    - pouco quantidade de serviços e sistemas na Internet

Cryptoviral Extortion

- **1996, apresentado na Conferência IEEE Security & Privacy, por Young e Yung, da Universidade de Columbia**

1. **Atacante gera um par de chaves assimétricas**
   - mantém a chave privada e inclui a chave pública no *ransomware*
2. **Atacante propaga o *ransomware***
3. **Vítima recebe e executa o *ransomware***
   - *ransomware* gera a chave simétrica, de forma randômica e a usa para criptografar os arquivos
   - chave simétrica é cifrada com a chave pública gerando ChaveRans
4. **Vítima recebe identificação (ChaveRans) e a informa ao pagar o resgate**
5. **Atacante decifra ChaveRans, usando a chave privada, e obtém chave simétrica**
6. **Atacante envia a chave simétrica à vítima**
7. **Vítima recebe a chave e a usa para decifrar os arquivos**

https://cacm.acm.org/magazines/2017/7/218875-cryptovirology/fulltext

História

- **2005 – novos casos começam a surgir**
- **2013 – CryptoLocker**
  - Operação Tovar (FBI, Europol e UK's National Crime Agency)
    - chaves privadas descobertas
  - código vazado levou ao surgimento de variantes
- **2014 – CryptoWall, CTB Locker**
- **2015 – TeslaCrypt**
- **2016 – Petya**

WannaCry (WannaDecryptor, WCry, WanaCrypt e WanaCrypt0r)

- **Maio/2017**
- **Explora vulnerabilidade no serviço SMBv1 da Microsoft (EternalBlue)**
  - *patches* lançados em 03/2017 (Boletim de Segurança MS17-010)
- **Utiliza módulo que permite a propagação (DoublePulsar)**
- **Possuía *kill switch* que permitiu que ele fosse contido inicialmente**
  - novas variantes surgem (Wannacry 2.0)
- **Microsoft lança *patch* para versões não mais suportadas**
- **Lições aprendidas:**
  - grande quantidade de máquinas desatualizadas
  - ausência de política de *backups*
  - serviços internos sendo acessados externamente

NotPetya (ExPetr/Petna)

- **Junho/2017**
- **Altera os setores de *boot* impedindo que o sistema inicie**
- **Pagamento não recupera os arquivos (Wiper)**
  - e-mail usado pelos atacantes foi bloqueado
- **Propagação (movimentação lateral):**
  - via ferramentas PsExec e WMIC
  - explorando vulnerabilidades do serviço SMBv1 (EternalBlue e EternalRomance)
- **Lições aprendidas:**
  - *firewall* não impede ataca
  - compartilhamentos de rede como vetor de ataque
  - ainda:
    - grande quantidade de máquinas desatualizadas
    - ausência de política de *backups*

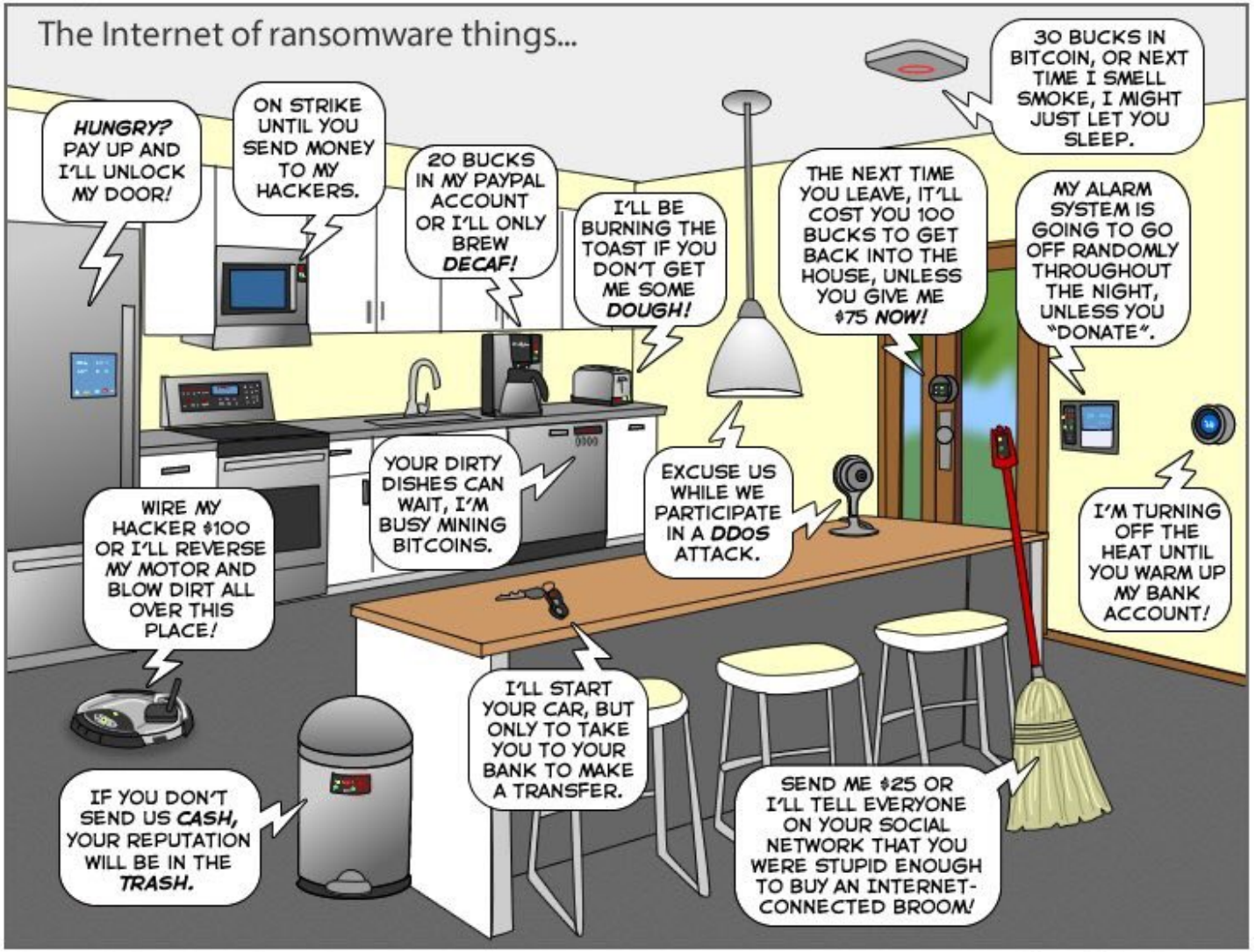
BadRabbit

- **Outubro/2017**
- **Vetor inicial: atualização do Adobe Flash Player**
- **Suspeita de ser uma variante do NotPetya**
- **Propagação via EternalRomance**

O que está por vir

- **RaaS**
- **Kits de ferramentas facilitam a criação de variantes**
- **Variação de preço conforme geolocalização**
- **Atacantes questionando se realmente vale a pena**
  - valor dos dados (extorsão)
- **IoRT (*Internet of Ransomware Things*)**
  - indisponibilidade de serviços

The Joy of Tech™ by Nitrozac & Snaggy



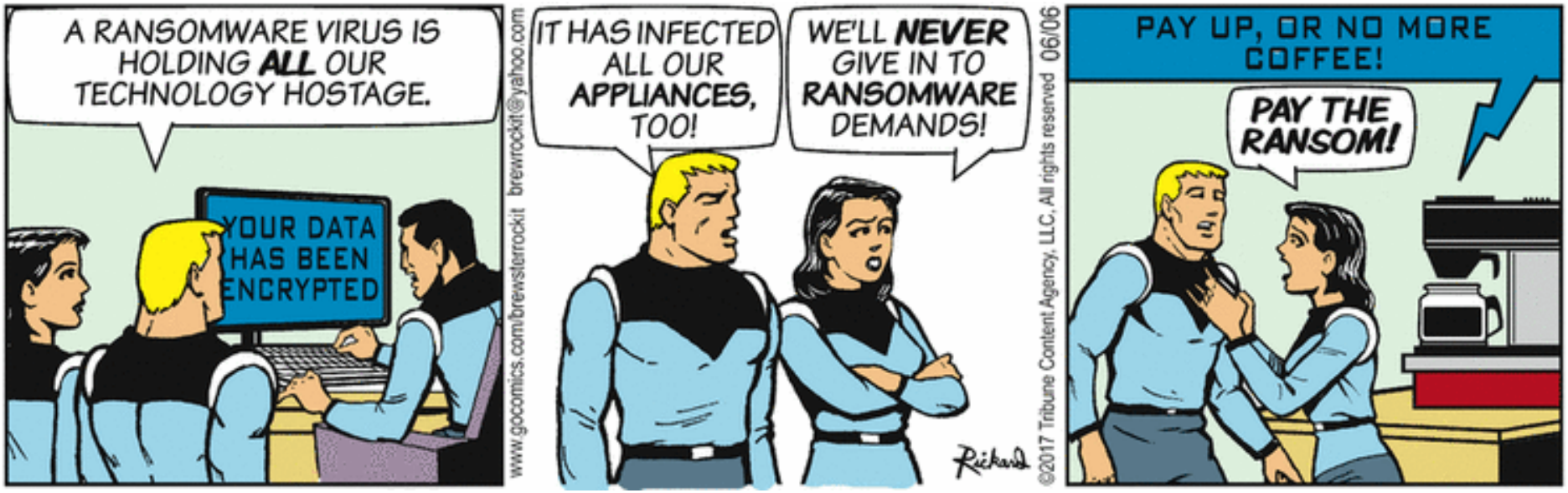
You can help us keep the comics coming by becoming a patron!
www.patreon/joyoftech

joyoftech.com

Dilema: Pagar ou não pagar o resgate

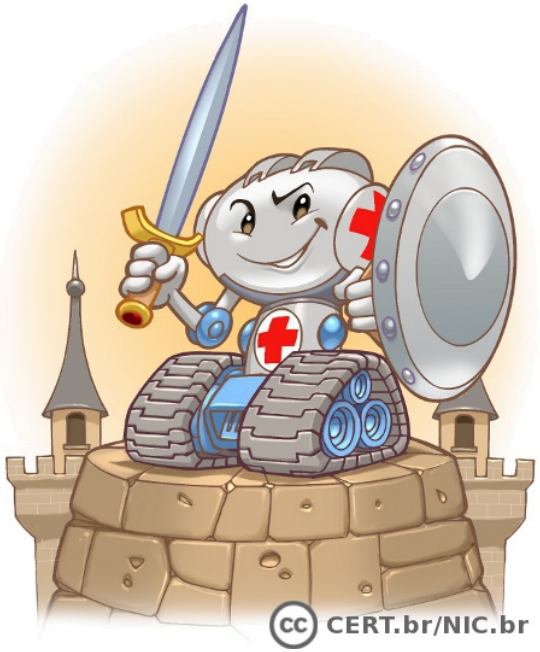
- **O que fazer se for infectado?**
  - tentar recuperar com alguma ferramenta
    - e cruzar os dedos ☹
  - esquecer os dados e se conformar ☹
  - pagar o resgate ☹☹
    - não garante a recuperação total
      - pode não haver comunicação com o atacante
    - incentivo ao crime
    - pode levar a outros pedidos de extorsão
  - recuperar o *backup* ☺☺☺

- **Melhor decisão**
  - não ter que decidir
  - prevenção é a melhor opção



https://www.peerlyst.com/posts/a-glimpse-of-the-future-iot-ransomware-business-model-eric-klein

Como se prevenir



Mantenha os equipamentos seguros

- **Instale a versão mais nova do sistema operacional**
- **Aplique todas as atualizações**
  - reinicie o equipamento sempre que solicitado
- **Desabilite os serviços desnecessários**
- **Instale antivírus e mantenha-o atualizado**
- **Use a conta de administrador do sistema apenas quando necessário**
  - a ação do *ransomware* será limitada às permissões de acesso do usuário que estiver acessando o sistema

Adote uma postura preventiva

- **Seja cuidadoso ao abrir arquivos anexos e ao clicar em *links***

- **Não considere que uma mensagem é confiável com base apenas em seu remetente**
  - remetente pode não ter checado a mensagem
  - pode ter sido enviada de:
    - conta falsa
    - conta invadida

Faça *backups* regularmente (1/4)

Backup é a solução mais efetiva contra _ransomware_

Faça *backups* regularmente (2/4)

- **Mantenha os *backups* atualizados**
  - de acordo com a frequência de alteração dos dados
- **Configure para que seus *backups* sejam realizados automaticamente**
- **Nunca recupere um *backup* se desconfiar que ele contém dados não confiáveis**
- **Mantenha os *backups* desconectados do sistema**
  - para que eles não sejam também criptografados
- **Faça cópias redundantes**
  - para evitar perder seus dados:
    - em incêndio, inundação, furto ou pelo uso de mídias defeituosas
    - caso uma das cópias seja infectada

Faça *backups* regularmente (3/4)
Redundância

"There are two kinds of people in the world:
those who have had a hard drive failure,
and those who will"
Peter Krogh

- **Quantas cópias manter?**
  - "quem tem um não tem nenhum"
- **Onde armazenar as cópias?**
- **Regra 3-2-1**
  - tenha pelo menos três cópias dos dados (uma primária e 2 *backups*)
  - armazene as cópias em duas mídias diferentes
  - mantenha ao menos uma das cópias *off-site* (ou ao menos *off-line*)

Faça *backups* regularmente (4/4)
Recuperação

- **Faça testes periódicos**
- **Certifique-se:**
  - de que eles estejam realmente sendo feitos
  - de conseguir recuperá-los

"No one cares if you can back up,

only if you can recover."

W. Curtis Preston - Unix Backup and Recovery

Conscientização de usuários

- **Campanhas internas de conscientização**
  - sobre a importância dos dados
  - sobre boas práticas de segurança

- **Participação dos funcionários são essenciais para a segurança da organização de forma geral**

Mantenha-se informado (1/2)

Cartilha de Segurança para Internet

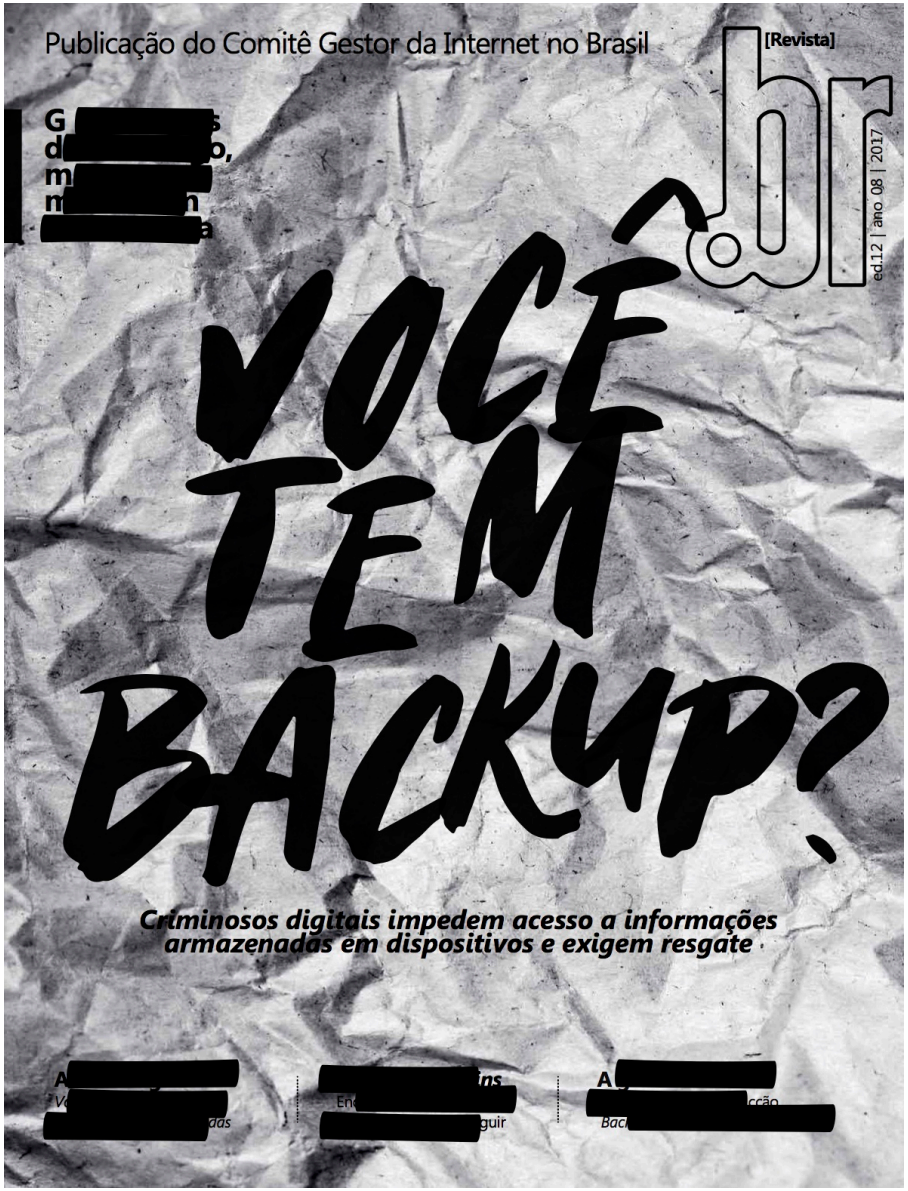
- https://cartilha.cert.br/

RSS

- https://cartilha.cert.br/rss/cartilha-rss.xml

Twitter

- http://twitter.com/certbr



http://nic.br/publicacao/revista-br-ano-08-2017-edicao-12/
https://cartilha.cert.br/


Você Tem
Backup?
Proteja seus dados, adote uma postura preventiva na Internet!
Entenda como o ransomware funciona, antes que seja tarde demais.
cartilha.cert.br
cert.br nic.br cgi.br

Obrigada

www.cert.br

miriam@cert.br

@cert

23 de novembro de 2017

nic.br cgi.br

www.nic.br | www.cgi.br